WHAT IS CLAIMED IS:

1. A method of controlling the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, the method comprising the steps of:

a. obtaining information associated with the network system;

b. setting one or more static policies for network services usage by the attached function;

c. setting one or more dynamic policies for network services usage by the attached function;

d. monitoring the network system for triggers; and

e. modifying the static policies, the dynamic policies, or both for the attached function based upon the monitored triggers.

2. The method as claimed in Claim 1 further comprising the step of saving set and modified policies associated with the attached function as policy history for the attached function.

3. The method as claimed in Claim 2 further comprising the step of querying whether a policy history exists for the attached function after obtaining the information from the network system.

4. The method as claimed in Claim 2 wherein the step of saving the set and modified policies associated with the attached function includes the step of caching some or all of the policy history in a network system device.

5. The method as claimed in Claim 4 further comprising the step of invalidating the cached policy history based upon the occurrence of a specified event.

6. The method as claimed in Claim 5 wherein the specified event is selected from the group consisting of time, size limitations, storage limits, a policy change, or a network system change.

7. The method as claimed in Claim 2 further comprising the step of evaluating whether the policy history includes any static policies that may be set for the attached function in a current session.

8. The method as claimed in Claim 1 wherein the triggers include timeouts, attached function changes, network infrastructure changes, intrusion detection events, firewall events, administrator inputs, network service changes and network service change requests.

9. The method as claimed in Claim 1 wherein the information includes attached function information, access device information, access port, number of devices per port, priority per port, priority per application, priority per device, application requested, exchange protocols available, port security, access location, and access time.

10. The method as claimed in Claim 1 wherein the only static policy is that there are only dynamic policies.

11. A method of controlling the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, the method comprising the steps of:

a. obtaining information associated with the network system;
b. setting one or more dynamic policies for network services usage by the attached function;
c. monitoring the network system for triggers; and
d. modifying the dynamic policies for the attached function based upon the monitored triggers.

12. The method as claimed in Claim 11 further comprising the step of saving set and modified policies associated with the attached function as policy history for the attached function.

13. The method as claimed in Claim 12 further comprising the step of querying whether a policy history exists for the attached function after obtaining the information from the network system.

14. The method as claimed in Claim 12 wherein the step of saving the set and modified policies associated with the attached function includes the step of caching the policy history in a network system device.

15. The method as claimed in Claim 14 further comprising the step of invalidating the cached policy history based upon the occurrence of a specified event.

16. The method as claimed in Claim 15 wherein the specified event is selected from the group consisting of time, size limitations, storage limits, a policy change, or a network system change.

17. The method as claimed in Claim 11 wherein the triggers include timeouts, attached function changes, network infrastructure changes, intrusion detection events, firewall events, administrator inputs, network service changes and network service change requests.

18. A system to control the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, the system comprising:

a. means, forming part of the network system, for obtaining information associated with the network system; and

b. a dynamic policy function module for setting static and dynamic policies for the attached function, for monitoring the network system for triggers, and for modifying the static policies, the dynamic policies, or both for the attached function based upon the monitored triggers.

19. The system as claimed in Claim 18 wherein the dynamic policy function module is a centralized module of a policy server of the network infrastructure.

20. The system as claimed in Claim 18 further comprising means for saving set and modified policies history.

21. The system as claimed in Claim 20 wherein the means for storing set and modified policies history forms part of the policy server of the network infrastructure.

22. The system as claimed in Claim 20 wherein the means for storing set and modified policies forms part of an interconnection device of the network infrastructure.

23. The system as claimed in Claim 18 wherein the dynamic policy function module is a distributed module forming portions of two or more devices of the network infrastructure.

24. The system as claimed in Claim 23 wherein the two or more devices are selected from a combination of one or more servers and one or more interconnection devices or a combination of two or more interconnection devices.

25. The system as claimed in Claim 20 wherein the means for saving set and modified policies includes means for caching the set and modified policies on a centralized network device, a local network device, or a combination of a centralized network device and a local network device.

26. The system as claimed in Claim 18 wherein the means for obtaining information associated with the network system includes IEEE 802.1X authentication, RADIUS authentication, or a combination of IEEE 802.1X authentication and RADIUS authentication of the attached function.

27. A system to control the usage by an attached function of network services of a network system that includes the attached function, one or more other attached functions and network infrastructure, the system comprising:

a. means, forming part of the network system, for obtaining information associated with the network system; and

b. a dynamic policy function module for setting dynamic policies for network services usage by the attached function, for monitoring the network system for triggers, and for modifying the dynamic policies for the attached function based upon the monitored triggers.

28. The system as claimed in Claim 27 wherein the dynamic policy function module is a centralized module of a policy server of the network infrastructure.

29. The system as claimed in Claim 27 further comprising means for saving set and modified policies history.

30. The system as claimed in Claim 27 wherein the dynamic policy function module is a distributed module forming portions of two or more network devices of the network infrastructure.

31. The system as claimed in Claim 27 further comprising means for caching set and modified policies history on one or more local network devices of the network infrastructure.

32. A system to control the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, based on one or more usage policies assigned to the attached function, the system comprising means for saving the assigned policies on a network device of the network infrastructure.

33. The system as claimed in Claim 32 wherein the means for saving the assigned policies is a distributed module forming portions of two or more devices of the network infrastructure.

34. A system to control the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and

network infrastructure, based on dynamic policies assigned to the attached function, the system comprising means for saving the assigned dynamic policies as policies histories.

35. The system as claimed in Claim 34 wherein the policies histories are saved on a policy server of the network infrastructure.

36. The system as claimed in Claim 34 wherein the policies histories are saved on one or more local network devices of the network infrastructure.

37. A system to control usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, based on one or more usage policies assigned to the attached function, the system comprising means for caching the assigned usage policies as policies histories.

38. The system as claimed in Claim 37 further comprising means for invalidating one or more of the cached policies histories based on a specified event.

39. The system as claimed in Claim 38 wherein the specified event is selected from the group consisting of time, size limitations, storage limits, a policy change, or a network system change.

40. A method of controlling the usage by an attached function of network services associated with a network system that includes the attached function, one or more other attached functions and network infrastructure, the method comprising the steps of:

a. setting one or more policies for network services usage by the attached function;
b. saving the one or more policies set as policies histories;
c. monitoring the policies histories for triggers; and
d. modifying the policies for the attached function based upon the monitored triggers.